

PKI/CAC Setup Procedures

The following pages contain instructions that will help you begin using and understanding the PKI/CAC. The first five steps must be completed only once.

Getting Started

Perform the following five steps in the given order to get started:

1. Get your card and PIN number
2. Secure and Use your card reader
3. Obtain & Install Root Certificates
4. Register digital Certificates
5. Set up Outlook

Using PKI/CAC

Be sure to read the following before sending a message

1. Learn PKI/CAC policies
2. Sending digital messages
3. Read digital messages/Obtain certificates from others
4. Sending encrypted messages
5. Read encrypted messages

What to do if you...

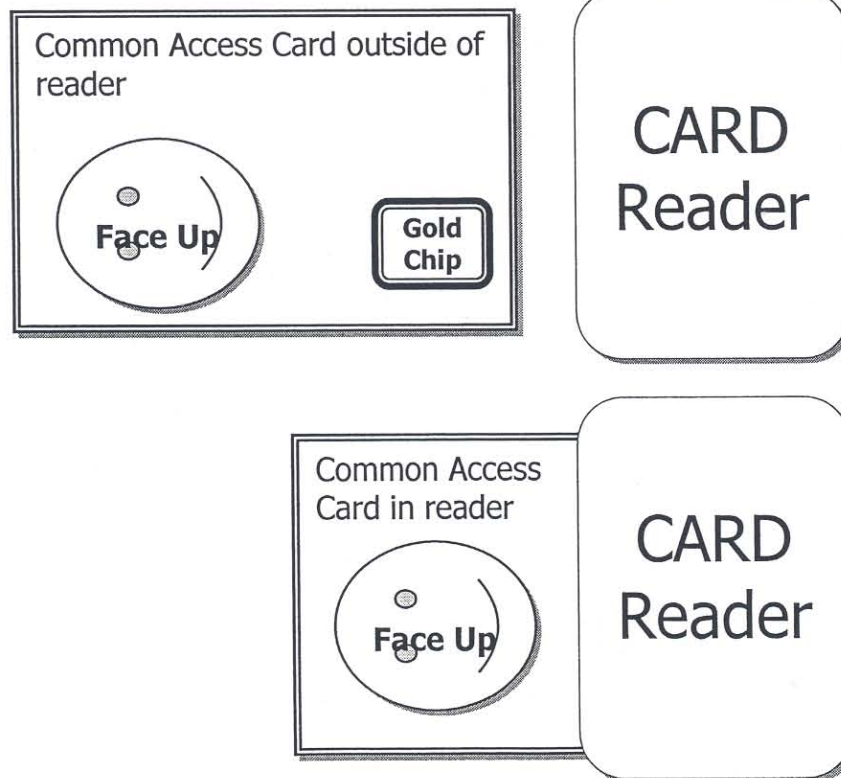
1. Lose your card
2. Forget your PIN number
3. Get locked out
4. Have problems with Card reader
5. Having problems with ActivCard Gold Utilities

Step 1 - Get your card and PIN number

1. Go to the DEERS office to pick up your card.
 - Located at the Codina Building
 - 8300 NW 33 Street, Suite 110, Room 17
 - Open Monday through Friday
 - Hours of operation: 1330-1530 (preferred time for SC Personnel).
 - Phone: (305) 437-2718
2. Fill out required documents.
3. Acquire PIN number (do not forget the number).
4. If you have problems with your card, return to the DEERS office.

Step 2 – Secure and Use CAC Card reader

1. There should be a CAC card reader located on or near the unclassified computer. If not, submit a work order.
2. Choose a place to mount the card reader that will remind you to remove your card every time you leave your workstation. Recommend moving it where you frequently see it and can use it more readily. Examples: underneath your monitor, on top of your monitor, or on your desk. Underneath the card reader are two adhesive strips. When removed the card reader will securely adhere to the place of your choice.
3. Select **Start > Programs > ActivCard > ActivCard Gold > ActivCard Gold Utilities**. (Or double click on the **ActivCard Gold Quick Fill button** located on the bottom right hand side of your screen to the right of the task bar.)
4. When prompted, insert your card face up into the card reader. The card reader will cover the gold chip but leave half of the card still displayed. (See illustration)
5. The green light on the CARD reader should start to blink.



6. When prompted **enter the PIN number**
7. Press **Enter**
8. **IMPORTANT:** You only get three attempts when prompted to type in your PIN number. After the third try you will be locked out and unable to send digital or encrypted messages. You will have to go back to the DEERS office to acquire another PIN number. They cannot unlock your account nor will they provide you with the number over the phone because it requires your fingerprint.
9. There will be no prompt on your screen recognizing the card is in the reader. This will be done when sending a signed or encrypted message.

Changing your PIN Number (optional)

1. If at some time you want to change your PIN number perform the following:
 - a. Select **Start > Programs > ActivCard > ActivCard Gold > ActivCard Gold Utilities**. (Or double click on the ActivCard Gold Quick Fill button located on the bottom right hand side of your screen to the right of the task bar.
 - b. When prompted **enter the PIN number**
 - c. Select **Tools > Change PIN**
 - d. **Type** in current PIN number then **type** in new desired PIN number twice **> Ok**
 - e. A message should appear stating the PIN was successfully changed.
 - f. Recommend testing the new PIN number by removing your card and redoing steps A and B.
 - g. Recommend testing the new PIN number by removing your card and redoing steps A and B.

Step 3 - Obtain & Install Root Certificates

1. Open **Internet Explorer** and type in the following web site address:
<http://dodpki.c3pki.chamb.disa.mil> > press **Enter**
2. On the left column of the web page, select **Download Root CA Certificates**
3. Scroll down then select **Download Class 3 Root CA Certificate**
4. Click **Save** (do not OPEN) > perform *all* of the following steps:
 - Select your **desktop** in the Save in field
 - Ensure Save as type is set to **All Files (*.*)**
 - CHANGE the file name to **DODROOT.P7B** then select the **Save** button.
 - When the message appears *download complete* select the **Close** button
5. Now select **Download Medium Assurance Root CA Certificate**
6. Click **Save** (do not OPEN) > perform *all* of the following steps:
 - Ensure Save as type is set to **All Files (*.*)** .
 - Select your **desktop** in the *Save in* field
 - CHANGE the file name to **DODROOTMED.P7B** then select the **Save** button
 - When the message appears *download complete* select the **Close** button
7. Close **Internet Explorer**
8. On your desktop, RIGHT CLICK (do not double click) on **DODROOT** and choose **Install Certificate**
9. Select **Next** on the *Certificate Import Wizard*
10. Accept the default *Automatically select the certificate based on the type of certificate*.
Select **Next** then **Finish** to complete the install process.
11. When prompted by a message, **do you want to ADD the following certificate to the root store?** Select **Yes**. When you see **The Import was successful**, select **OK**
12. Repeat the steps 8-11 substituting **DODROOTMED.P7B**.
13. Right click on **DODROOT** > delete > yes. Right click on **DODROOTMED** > delete > yes. You have successfully imported your root certificates.

Step 4 - Register digital Certificates

1. Select **Start > Programs > ActivCard > ActivCard Gold > ActivCard Gold Utilities**.
2. The program will prompt you to insert your **CAC** into the card reader.
3. Insert your card > When prompted, click **OK**.
4. When prompted, enter your **PIN** and click **OK**. (Warning: you have three attempts until locked out. If you get locked out you will have to go back to the DEERS office to get a new PIN number.)
5. Click the **+** sign next to Digital Certificates to expand the **Digital Certificates** folder
6. Select the **Certificate** that is bold
7. From the menu bar, select **Tools > Register Certificates**.
8. Click **Yes** to proceed.
9. Click **OK** to complete Certificate installation. Your certificates are now successfully registered. (NOTE: All 3 certificates will be registered in this one step.)
10. Click the **Close** button to close the ActivCard Gold Utilities window.

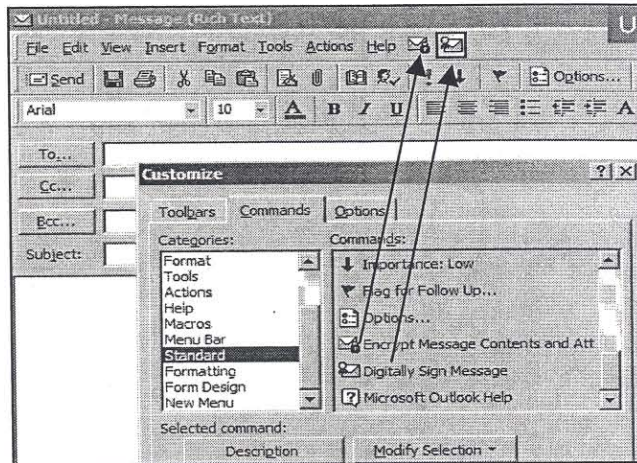
Step 5 - Set up Outlook

1. Insert the **CAC** into the card reader if it is not already inserted.
2. Open Microsoft **Outlook**.
3. Select **Tools > Options** > select **Security** tab then click on the **Settings** button.
4. In the *Security Settings Name* field, type your first and last name (Example: John Doe, not case sensitive)
5. Ensure **S/MIME** is selected in the *Secure Message Format* field.
6. Ensure the checkbox next to *Default Security Settings for the Secure Message Format* is selected
7. Ensure the checkbox next to *Default Security Settings for all secure messages* is selected.
8. To the right of *Signing Certificate*, click the **Choose** button.
9. Double click the line between **Issued by** and *Intended* columns to expand the columns and see its contents.
10. Highlight the certificate that starts with **DOD CLASS 3 EMAIL ...** Click **OK**.
11. Ensure that **SHA1** is selected in the Hash Algorithm drop down menu.
12. To the right of *Encryption Certificate*, click the **Choose** button.
13. Double click on the line between *Issued by* and *Intended* columns to expand the columns.
14. Highlight the Certificate that starts with **DOD CLASS 3 EMAIL**. Click **OK**.
15. Ensure **3DES** is selected in the *Encryption Algorithm* drop down menu. Click **OK**.
16. At the top under *Secure Email*, enable the check box next to **Add digital signature to outgoing messages**.
17. Ensure that the **Send clear text signed message** check box is also enabled. Click **OK**.
18. Open a New Message. Maximize the window (if needed.)

19. Click **View > Toolbars > Customize**. Select the **Commands** tab. Select **Standard** under the **Categories** menu.

20. On the right side, scroll through the list of commands to find and select **Encrypt Message Contents and Attachments**.

21. Drag and drop this icon to the right hand side of **HELP** on your menu bar at the top of your screen. (See illustration)



22. Continue to scroll through the commands. Locate and select the **Digitally Sign Message** icon.

23. Drag and drop this icon to the right of the encrypt icon you just placed on your menu bar.

24. **Close** the Customize window.

25. Close the Message. Open a new message. Notice both icons appear on your menu bar and the digitally signed icon is activated. This will occur every time you open a New Message. Close the message.

26. Select **Tools** then **services**. Select the **Addressing** tab.

27. Under *keep personal addresses in*, be sure **contacts** are selected.

28. Under *When sending mail*, select **contacts** and then using the arrow on the right move it to the top of the list. (NOTE: If contacts are not listed, select Add locate Contacts then add it.) Click **Ok**.

Learn CAC card policies

1. As of October 1st, 2003, SOUTHCOM personnel who have unclassified email accounts and operational CAC cards must digitally sign all messages sent from unclassified to unclassified email accounts. Those personnel who have not obtained their CAC cards and are not operational, have a six-month grace period.
2. Always remove your CAC card from the card reader when leaving your workstation.
3. Do not digitally sign messages when emailing classified accounts. Email sent from a classified machine will not contain a digital signature.
4. Although encryption is possible, it is not required.
5. When receiving encrypted mail the implication is that it contains Sensitive but Unclassified information that needs to be protected during transmission.
6. Encrypted mail received should not be forwarded in an unencrypted format.
7. It takes about 10-15 minutes to issue a card. Other important reminders: -
 - a. CACs (ID-cards) are property of the US Government.
 - b. When these cards expire or become worn out, they are to be turned- in to the nearest ID-card issuing facility.
 - c. You are not allowed to destroy and discard them yourself--these cards have to be accounted for 100 percent.
 - d. The CAC itself is not to be punch-holed, mutilated or placed next to credit cards, etc. Daily care of the CAC is important.
 - e. Contractor personnel must present a completed DD Form 1172-2 signed by the appointed Verifying Official (VO). Copy of the VO letter of appointment must be filed in the ID-DEERS office.

Sending digital messages

Things to know:

1. Send all messages digitally signed from unclassified to unclassified addresses
2. Do not send a signed message from unclassified to classified email accounts

How to send a signed message:

1. Start a new message in Outlook (**File > New > Mail Message**)
2. Compose the message as usual
3. Before sending you will notice the Digitally Sign Message button is activated
4. Send the message (using the **Send** button or the keyboard shortcut **Alt + S**)
5. If your CAC card is not in the reader, you will be prompted to **insert it** and then **enter your PIN number** then click **OK**.
6. To verify you digitally signed the message, go to **Sent Items**. Locate the message you sent. Open the message. On the right side, you will see a red ribbon displayed.
7. You can click on the red ribbon to view more information about the digital signature.
8. After the message is successfully sent, **remove your CAC card** from the reader.



Digital signature icon

Reading digitally signed messages/Obtaining certificates

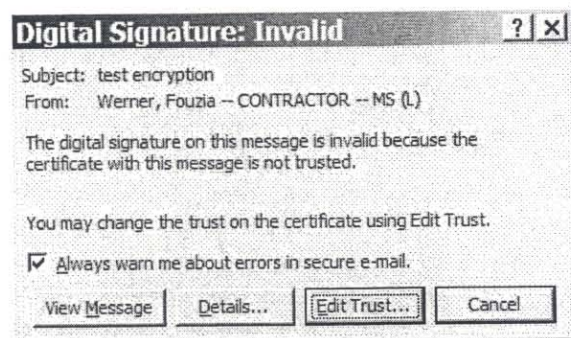
Things to know:

- Before sending an encrypted message you must obtain the recipients certificate
- Obtaining certificates occurs when an individual sends you a message with a digital signature

How to obtain a certificate from a digitally signed message

1. Open a message that has been digitally signed  Digitally signed message

2. The following message will appear. (If you do not see this message you have set the trust level on the certificate associated with this signature to view messages directly.)



3. Select the **Edit Trust** button.

NOTE: It is recommended you

Edit Trust first to validate this signature came from a source you trust.

4. On the **Trust** tab you can perform one of the following:
 - (1) If you trust the person sending the message (e.g. SC personnel) and expect more signed messages from them, select **Explicitly Trust this Certificate**. Future messages signed with this certificate will not require you to re-edit the trust.
 - (2) Otherwise, you can choose *Inherit Trust from Issuer* and *Explicitly Don't Trust this Certificate* that will continue to prompt you before opening a message. On the **General/Details** tabs you can learn more about the person's certificate. Certificates that show the issuer is DOD CLASS means they were provided by the Department of Defense.
5. When you select the **View Message** button you will be able to read the message directly.

Obtain Certificate


6. If you trust the source, obtain their certificate by **Right Clicking** on their name in the message header next to **FROM**. Then select **Add to Contacts**. You can add additional information under File As (e.g. Last Name, First).
7. Select the **Certificates** tab. Verify their certificate is displayed. Select **Save and Close**. You can close the message.

Sending encrypted messages

Things to know:

- Before sending an encrypted message you must have obtained the recipients certificate
- Encrypted messages should be the exception rather than the rule. Although encryption is possible, it is not required.
- Send all messages encrypted from unclassified to unclassified addresses
- Do not send an encrypted message from unclassified to classified email accounts

How to send an encrypted message:

1. Start a new message in Outlook (**File > New > Mail Message**)
2. You must select the address from your Contacts not the Global Address List. Select the **To...** Button to open the address book.
3. Change address book to contacts. Next to the **Show Names from the:** select Contacts.
4. Locate the desired name(s) then click **OK**.
5. Compose the subject and body of the message as usual
6. Before sending you will notice the Digitally Sign Message button is activated
7. Select the **Encrypted Icon**  *Encrypted Message Contents Icon*
8. Send the message (using the **Send** button or the keyboard shortcut **Alt + S**). If you get an error message read the troubleshooting tips.
9. If your CAC card is not in the reader, you will be prompted to **insert it** and then **enter your PIN number** then click **OK**.



Digital signature icon



Encrypted Message Contents Icon

10. After the message is successfully sent, **remove your CAC card** from the reader.

Reading Encrypted messages

1. Open the message. You should see the encrypted icon on the message.
2. You will be required to insert your CAC card into the reader, enter your PIN and then be able to view the message.

What to do if you...

- *Lose your card* – Call the DEERS office (Codina Building) immediately 437-2718.
- *Forget your PIN number* – Must go in person to DEERS office to get a new PIN number reissued.
- *Get locked out* – You are provided three attempts to use your CAC card with the PIN. After the third try, you will get a message saying you are locked out. You must go in person to the DEERS office to a new PIN number. You cannot phone or email to get unlocked.
- *Have problems with your card reader*— call the Help Desk 437-1234.
- *Have problems with ActivCard Gold Utilities software*— call the Help Desk 437-1234.